

This Listing of Claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A Video-on-Demand method for demanding a video program via a short message, comprising the steps of:

generating, at a user end, a demand short message including information on the demanded video program, said demand short message including at least a User Identifier field, a Program Identifier field of the demanded video program and an Authentication field;

encrypting the fields in the generated demand short message except the Authentication field at the user end;

sending said encrypted fields and not encrypted Authentication field in the generated demand short message to a demand processing means at [[, to]] a program delivering end where an Authentication field is calculated, the generated demand short message; said sending including communicating said generated demand short message via a wireless communication from a mobile phone device;

receiving the demand short message at the program delivering end, decrypting and processing the short message to extract the user identifier and the program identifier and ~~using~~ comparing the calculated Authentication field with the received non-encrypted Authentication field to authenticate legality of the user when said two fields are identical;

after authenticating the legality of the user successfully, sending program content corresponding to a program identifier from the program delivering end to the user end indicated by the user identifier; and

receiving the demanded video program at the user end.

2. (Original) A Video-on-Demand method according to claim 1, further comprising the step of sending from the program delivering end to the user end a reply message including a confirmation message indicating that the demand short message has been received.

3. (Cancelled)

4. (Original) A Video-on-Demand method according to claim 1, wherein said demand short message further comprising:

- a Format Identifier field for defining a format of said demand short message;
- a Demand Time field for indicating a time for sending said demand;
- a Playback Time field for indicating a start time of video playing;
- an Optional field containing optional data that may describe said demand more precisely; and

said Authentication field is an encrypted digest of the above User Identifier field, Program Identifier field, Format Identifier field, Demand Time field, Playback Time field, and Optional field.

5. (Original) A Video-on-Demand method according to claim 4, wherein said Authentication field is generated according to the following procedure:

- calculating the digest of all the fields except the Authentication field using a digest algorithm;

- encrypting with a cipher algorithm a calculated digest by adopting a secret authentication key corresponding to a user end device, uniquely allocated in advance by the program delivering end; and

- a process of authenticating a user's legality by the program delivering end being conducted according to the following procedures:

- calculating the digest of all the fields except the Authentication field using a digest algorithm;

- encrypting with a cipher algorithm the calculated digest by adopting a secret authentication key corresponding to a user end device, uniquely allocated in advance by the program delivering end, so as to calculate an Authentication field; and

- checking whether the calculated Authentication field and the received Authentication field are identical.

6. (Original) A Video-on-Demand method according to claim 5, wherein when said video program is sent via a conditional access system, a content key is delivered with the video program, so there is no need for a separate deliver of said reply message.

7. (Original) A Video-on-Demand method according to claim 5, wherein when the video program demanded by the user needs to be encrypted and the encrypt key is not sent via a conditional access system, the method further comprising the steps of:

generating, at the program delivering end, an encrypted reply message containing a content key of said video program, and sending it to the user end;

decrypting, at the user end, the content key from said encrypted reply message; and

decrypting the video program received from the program delivering end according to the decrypted content key.

8. (Original) A Video-on-Demand method according to claim 7, wherein said encrypted content key is encrypted using a device key corresponding to the user end device, uniquely allocated in advance by the program delivering end, and said device key can be different from said Authentication key.

9. (Currently Amended) A Video-on-Demand system for demanding a video program via a short message, comprising:

short message generating means for receiving a user demand, and generating a demand short message based on the user demand, said demand short message including at least a User Identifier field, a Program Identifier field of the demanded video program and an Authentication field, and including an encrypting unit for encrypting the fields in the generated demand short message except the Authentication field;

short message sending means for sending the demand short message generated by the short message generating means, said short message sending means comprising a mobile phone device for sending said demand short message via a wireless connection;

demand short message processing means at a program delivering end for receiving the demand short message and the Authentication field, processing the received demand short message to calculate an Authentication field, comparing the calculated Authentication field with

~~the received to extract the user identifier and using the Authentication field to authenticate the~~
legality of the user when said two fields are identical, and sending the program identifier of the
demanded program by a legal user to video delivering means, and including decrypting means
for decrypting the received encrypted short message;

video delivering means for sending program content corresponding to the program
identifier from the program delivering end to the user end indicated by a legal user identifier; and

program playing means at the user end for receiving the video program sent by the video
delivering means and playing it back to the user.

10. (Original) A Video-on-Demand system according to claim 9, wherein the demand short
message processing means further comprises a reply message generating unit for generating a
reply message including at least a confirmation message indicating that the demand short
message has been received, for sending to the user end.

11. (Cancelled)

12. (Original) A Video-on-Demand system according to claim 9, wherein said short message
generating means further comprises a program information generating unit for generating said
User Identifier field, said Program Identifier field of the video program demanded by the user
and

a Format Identifier field for defining a format of said demand short message,
a Demand Time field for indicating a time for sending said demand,
a Playback Time field for indicating a start time of video playing, and
an Optional field containing optional data that may describe said demand more
precisely.

13. (Original) A Video-on-Demand system according to claim 12, wherein

said short message generating means further comprises an Authentication field
generating unit for calculating a digest of all the fields except the Authentication field
using a digest algorithm and encrypting with a cipher algorithm the calculated digest by
adopting a secret authentication key corresponding to a user end device, uniquely

allocated in advance by the video delivering means; and

said demand short message processing means further comprises an authentication unit for calculating the digest of said User Identifier field, Program Identifier field, Format Identifier field, Demand Time field, Playback Time field and Optional field, encrypting with a cipher algorithm the calculated digest by adopting a secret authentication key corresponding to a user end device, uniquely allocated in advance by the video delivering means, so as to calculate an Authentication field and checking whether the calculated Authentication field and the received Authentication field are identical.

14. (Original) A Video-on-Demand system according to claim 13, wherein if said video program is sent via a conditional access system, a content key is delivered with the video program.

15. (Original) A Video-on-Demand system according to claim 13, wherein if the video program demanded by the user needs to be encrypted and the encrypt key is not sent via a conditional access system, then the demand short message processing means generates an encrypted reply message containing a content key of said video program, and sends it to the user end; and

the program playing means at the user end decrypts the content key from said encrypted reply message, and decrypts the video program received from the program playing means according to the decrypted content key.

16. (Original) A Video-on-Demand system according to claim 15, wherein said encrypted content key is encrypted using a device key corresponding to the user end device, uniquely allocated in advance by the program delivering end, and said device key can be different from said Authentication key.

17. (Currently Amended) Short message generating means in a Video-on-Demand system, comprising:

a receiving unit for receiving a user demand;

a program information generating unit for generating, according to the user

demand, program information including at least a User Identifier field and a Program Identifier field of the demanded video program;

an Authentication field generating unit for generating a Authentication field according to the program information generated by the program information generating unit;

an encrypting unit for encrypting the fields except the Authentication field in the demand short message; [[and]]

an output unit for outputting said program information and the Authentication field as a demand short message to a short message sending means;

sending said demand short message to a demand short message processing means at a program delivering end for calculating an Authentication field, and comparing the calculated Authentication field with the received Authentication field in the demand short message to authenticate legality of the user when said two Authentication fields are identical.

18. (Cancelled)

19. (Original) A short message generating means according to claim 17, wherein said program information generating unit further generating:

a Format Identifier field for defining a format of said demand short message,
a Demand Time field for indicating the time for sending said demand,
a Playback Time field for indicating the start time of video playing, and
an Optional field containing optional data that may describe said demand more precisely.

20. (Original) A short message generating means according to claim 19, wherein said Authentication field generating unit calculates the digest of all the fields except the Authentication field using a digest algorithm and encrypts with a cipher algorithm the calculated digest by adopting a secret authentication key determined in advance and uniquely corresponding to said short message generating apparatus.

21. (Original) A short message generating means according to claim 20, wherein said digest algorithm is MD5 algorithm, and said cipher algorithm is 3DES algorithm.

22. (Currently Amended) A short message generating method in a Video-on-Demand system, comprising the steps of:

receiving a user demand;

generating, according to the user demand, program information including at least a User Identifier field and a Program Identifier field of a demanded video program;

generating an Authentication field according to the generated program information;

encrypting the generated program information; and

outputting said encrypted, generated program information and the Authentication field as a demand short message to a short message sending means comprising a mobile phone device for sending said demand short message via a wireless connection to a demand short message processing means at a program delivering end where an Authentication field is calculated, and comparing the calculated Authentication field with the received Authentication field in the demand short message to authenticate legality of the user when said two Authentication fields are identical.

23. (Cancelled)

24. (Currently Amended) A demand short message processing method in a Video-on-Demand system, comprising the steps of:

~~Receiving~~ receiving, via a wireless connection, a demand short message having encrypted fields and an Authentication field that is not encrypted ~~generated~~ sent by a mobile phone device;

decrypting the demand short message;

calculating an Authentication field from the decrypted demand short message;

~~extracting a user identifier~~ an Authentication field from the decrypted demand short message;

comparing the calculated Authentication field with the extracted Authentication field in the demand short message to authenticate legality of a user when said two Authentication fields are identical;

~~authenticating legality of a user identified by the extracted user identifier, according to the Authentication field in the decrypted demand short message; and~~

outputting a program identifier of the program which the legal user demands.

25. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing Video-on-Demand, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

26. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for Video-on-Demand, said method steps comprising the steps of claim 1.

27. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing Video-on-Demand, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 9.

28. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing short message generation, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 17.

29. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing short message generation, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 22.

30. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for short message generation, said method steps comprising the steps of claim 22.

31. (Cancelled)

32. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing demand short message processing, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 24.

33. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for demand short message processing, said method steps comprising the steps of claim 24.

34. (Previously Presented) The Video-on-Demand method according to claim 1, wherein a sum of the lengths of the fields do not exceed 100 bytes.

35. (Previously Presented) The Video-on-Demand system according to claim 9, wherein a sum of the lengths of the fields do not exceed 100 bytes.

36. (Previously Presented) The Short message generating means in a Video-on-Demand system according to claim 17, wherein a sum of the lengths of the fields do not exceed 100 bytes.

37. (Previously Presented) The short message generating method in a Video-on-Demand system according to claim 22, wherein a sum of the lengths of the fields do not exceed 100 bytes.